UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,158	07/22/2003	Jeffrey S. Bardsley	9407-2	7454

20792 7590 11/09/2007

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
TOLENTINO, RODERICK	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
11/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/624,158
Filing Date: July 22, 2003
Appellant(s): BARDSLEY ET AL.

D. Randal Ayers (40,493)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 08/17/2007 appealing from the Office action mailed 04/27/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner.

(1) Rejection of Claims 4 – 7, 14 – 17 and 22 under 35 U.S.C. 103(a) which have been designated as part of Argument sections 'D' and 'E' by Appellant have been withdrawn. Arguments in regards to these rejections have been found persuasive. Claims 4 – 7, 14 – 17 and 22 are objected to as being dependent upon a rejected base

claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

7,073,198	Flowers et al.	07-2006
2004/0006704	Dahlstrom et al.	01-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1 – 3, 8 – 13 and 18 – 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flowers et al. U.S. Patent No. (7,073,198) in view of Dahlstrom et al. U.S. PG-Publication No. (2004/0006704).

As per claims 1, 11 and 21, Flowers teaches establishing a baseline identification of an operating system type and an operating system release level for the computer system that is compatible with a Threat Management Vector (TMV) (Flowers, Col. 4 Lines 26 – 37) but fails to teach receiving a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type and an operating system release level and processing countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release

level for the computer system as being affected by the computer security threat. However, in an analogous art Dahlstrom teaches receiving a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type (Dahlstrom, Paragraph 0006) and an operating system release level and processing countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat (Dahlstrom, Paragraph 0042).

At the time the invention was made, it would have been obvious to use Dahlstrom's system for determining security vulnerabilities with Flowers' method for detecting vulnerability in a network because it offers the advantage of properly having ways to fix detected vulnerabilities.

As per claims 2 and 12, Flowers as modified teaches comprises receiving a TMV history file in response to installation, configuration or maintenance of the computer system (Dahlstrom, Paragraph 0018) and wherein the processing comprises processing countermeasures that are identified in the TMV history file (Dahlstrom, Paragraph 0006, record of fixes).

As per claims 3 and 13, Flowers as modified teaches updating a threat management information base for the computer system to account for the countermeasures that are processed file (Dahlstrom, Paragraphs 0027 and 0036).

As per claims 8 and 18, Flowers as modified teaches the set of possible countermeasures comprises an identification of a countermeasure mode of installation (Dahlstrom, Paragraphs 0044 and 0042).

As per claims 9 and 19, Flowers as modified teaches the receiving comprises pruning at least some of the TMV to discard at least some of the TMV that is not needed for processing countermeasures (Dahlstrom, Paragraph 0027).

As per claims 10 and 20, Flowers as modified teaches the receiving comprises mutating the TMV that is received to a format that is compatible with processing countermeasures (Dahlstrom, Paragraph 0042).

(10) Response to Argument

Response to Section A) of Argument

Appellant argues on pages 5 – 8 of the Appeal Brief filed 8/17/2007, that Flowers in view of Dahlstrom fails to teach receiving a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type and an operating system release level and processing countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat. Examiner respectfully disagrees. Flowers teaches establishing a baseline identification

of an operating system type and an operating system release level for the computer system that is compatible with a Threat Management Vector (TMV) (Flowers, Col. 4 Lines 26 – 37) and in an analogous art Dahlstrom teaches receiving a TMV including therein a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type and a third field that provides identification of a set of possible countermeasures for an operating system type (Dahlstrom, Paragraph 0006) and an operating system release level and processing countermeasures that are identified in the TMV if the TMV identifies the operating system type and operating system release level for the computer system as being affected by the computer security threat (Dahlstrom, Paragraph 0042).

According to the specification of the case, A TMV is described as a first field that provides identification of at least one operating system type that is affected by a computer security threat, a second field that provides identification of an operating system release level for the operating system type, and a third field that provides identification of a set of possible countermeasures for an operating system type and an operating system release level. A TMV is merely just information that pertains to a system and its possible countermeasure. Flowers teaches the fields that identify the operating system and identify the release level, in Col. 4 Lines 26 – 37 of Flowers. Flowers shows the identification of an operating system, and the release level is merely Flowers, has taught the information regarding the operating system being used and what version of the operating system is being used. Dahlstrom, teaches identifying the

operating system, and from there determining the vulnerabilities that pertain to the operating system and in turn determining the countermeasures to protect against the vulnerabilities. From here the information pertaining to the vulnerabilities and countermeasures for the operating are sent to the computer system.

Response to Section B) of Argument

Appellant argues on pages 8 – 9 of the Appeal Brief filed 8/17/2007, that Flowers in view of Dahlstrom fails to teach receiving a TMV history file in response to installation, configuration or maintenance of the computer system and wherein the processing comprises processing countermeasures that are identified in the TMV history file. Examiner respectfully disagrees. Flowers as modified teaches receiving a TMV history file in response to installation, configuration or maintenance of the computer system (Dahlstrom, Paragraph 0018) and wherein the processing comprises processing countermeasures that are identified in the TMV history file (Dahlstrom, Paragraph 0006, record of fixes). Dahlstrom shows that it has countermeasure information pertaining to certain operating systems. This in itself is history data. The information for operating systems is information that it is based on known vulnerabilities in a system. It is not information that is going to be used on future unknown vulnerabilities. The fact that the information is based on known data, would be known to anyone of ordinary skill in the art to be history data.

Response to Section C) of Argument

Appellant argues on page 9 of the Appeal Brief filed 8/17/2007, that Flowers in view of Dahlstrom fails to teach updating a threat management information base for the computer system to account for the countermeasures that are processed file. Examiner respectfully disagrees. Flowers in view of Dahlstrom teaches updating a threat management information base for the computer system to account for the countermeasures that are processed file (Dahlstrom, Paragraphs 0027 and 0036).

Dahlstrom on paragraph 0027 teaches,the automated or manual update of a product record. The product record is the file of information, in this case countermeasure information that coincides with the product, in this case the operating system is the product. By updating the information the, the threat management information of the system and it's operating system will be updated with countermeasures for the operating system.

Response to Section F) of Argument

Appellant argues on pages 11 – 12 of the Appeal Brief filed 8/17/2007, that Flowers in view of Dahlstrom fails to teach the receiving comprises pruning at least some of the TMV to discard at least some of the TMV that is not needed for processing countermeasures. Examiner respectfully disagrees. Flowers in view of Dahlstrom teaches the receiving comprises pruning at least some of the TMV to discard at least some of the TMV that is not needed for processing countermeasures (Dahlstrom, Paragraph 0027).

Dahlstrom teaches an automated update, anyone of ordinary skill in the art would know that an update will bring in new information and any old information that has been outdated will be discarded and replaced.

Response to Section G) of Argument

Appellant argues on page 12 of the Appeal Brief filed 8/17/2007, that Flowers in view of Dahlstrom fails to teach the receiving comprises mutating the TMV that is received to a format that is compatible with processing countermeasures. Examiner respectfully disagrees. Flowers in view of Dahlstrom teaches the receiving comprises mutating the TMV that is received to a format that is compatible with processing countermeasures (Dahlstrom, Paragraph 0042).

Dahlstrom shows that different products have different relevant data. Thus information sent to different systems will be sent in a format that is compatible to the system, all based on the data relevant to the system.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Roderick Tolentino

Conferees:

Kambiz Zand

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Kim Vu